UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/724,972	11/28/2000	Stephen M. Trimberger	X-805-9 US	7821

24309 7590 04/21/2006

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/724,972	**Applicant(s)** TRIMBERGER ET AL.	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,8-13,16-23,26 and 27* is/are rejected.

7)☒ Claim(s) *5,6,14,15, 19, 24, 25 and 28* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated February 3, 2006. Claims 1-28 are pending.

Response to Arguments

2. Applicant's arguments filed February 3, 2006 have been fully considered but they are not persuasive. Applicant argues Yip does not disclose using address data from an address indicator in a decryption algorithm. Along with applicant's confirmation that Yip describes a secret sequence (i.e. key) is read from nonvolatile memory, the examiner contend that in (nonvolatile) memory, address is a number (i.e. a pointer or an index) specifying a location where data is stored (inherently understood in the computer system) and Yip discloses a decryption algorithm using data (i.e. key) from the address indicator for decrypting the encrypted bitstream (page 3, paragraph [0031]). Applicant also argues that Yip does not teach decrypting using an address (remarks, page 9). In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 8-10, 16-17 and 26-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Yip (2001/0032318).

a) As to claim 1, Yip discloses an apparatus and method for protecting configuration data in a programmable device comprising a decryptor for decrypting an encrypted bitstream (Fig. 1, element 21); an address indicator for indicating an address into which configuration data will be loaded (page 4, paragraph [0032]; Fig. 2, element 42); and a decryption algorithm implemented by the decryptor, wherein the decryption algorithm uses data (Fig. 2, element 48) from the address indicator for decrypting the encrypted bitstream (page 3, paragraph [0031]).

b) As to claims 8-10, 16-17 and 26-27, Yip discloses a value in the bitstream is loaded in the address indicator (Fig. 4; page 4, paragraphs [0036-0039]), wherein the value is encrypted (claims 9, 16 and 26) or unencrypted (claim 10, 17 and 27).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2, 4, 12-13 and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yip et al. (2001/0032318) in view of Kean (US 2001/0015919).

a) As to claims 2, 12 and 22, Yip does not disclose the address indicator is an initial address indicator.

Kean discloses the address in the configuration bitstream indicates an initial address in configuration memory at which configuration data is to be stored (page 7, paragraph [0098]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the address indicator is an initial address indicator in the system of Yip as Kean teaches so as to place data at a specific location.

b) As to claims 4, 13 and 23, Kean discloses the PLD wherein the decryption algorithm comprises the DES algorithm (page 2, paragraph 0020).

7. Claims 11, 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kean (US 2001/0015919) in view of Yip et al. (2001/0032318).

a) As to claims 11 and 20, Kean discloses a method and apparatus for secure configuration of a field programmable gate array (FPGA) comprising storing a plurality of decryption keys in storage elements of the PLD (i.e. multiple keys in triple DES where they are stored in ID register, in nonvolatile memory, page 2, paragraphs [0012], [0015], [0019-0021]); receiving a configuration bitstream at the PLD, wherein the configuration bitstream includes control data (Fig. 6, elements 80-84) and configuration data (Fig. 6, element 86) and at least the configuration data is encrypted (page 2, paragraph [0011]); decrypting the configuration bitstream in the PLD using the plurality of decryption keys whereby a decrypted configuration bitstream is generated (Fig. 5, element 64; page 1, paragraph [0009]; page 8, paragraphs 0104-0107). Kean discloses the security circuit (Fig. 5, element 64) may encrypts/decrypts the configuration data using the triple data encryption standard algorithm (i.e. plurality of decryption keys) in a cipher block chaining (CBC) mode algorithm (page 2, paragraphs [0015] and [0023]). Kean further discloses cipher block chaining mode with the required initial value saved as part of the header before the configuration information (page 8, paragraphs [0107-0112] and in CBC decryption, the initial value is used for starting the chaining; and storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD page 7, paragraph [0095]).

However, Kean does not disclose decrypting the configuration bitstream in the PLD using the address from the configuration bitstream.

Yip discloses decrypting the configuration bitstream in the PLD using the address from the configuration bitstream (page 3, paragraph [0031]; Fig. 2, element 48).

Yip and Kean do not disclose control data includes an address that references configuration memory of the PLD.

The admitted prior art discloses control data includes an address that references configuration memory of the PLD. (Fig. 2d).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of control data including an address in referencing configuration memory of the PLD, as admitted prior art teaches, in the system of Kean and Yip so as to indicate the types of control information that can be loaded into the registers.

b) As to claim 18, Kean does not disclose disabling readback of configuration data from the PLD after storing the configuration data in configuration memory.

However, Kean discloses reading back of configuration data with an encryption key to form a secure bitstream (page 6, paragraph [0072]). This concept of securely protect configuration data would be implemented as to disable readback of configuration data after storing the configuration data in configuration memory.

8. Claims 3 and 21are rejected under 35 U.S.C. 103(a) as being unpatentable over Kean (US 2001/0015919) in view of Yip et al. (2001/0032318).

a) As to claim 21, Kean discloses a programmable logic device comprising a configuration memory (Fig. 5, element 14); a key management circuit adapted for storage of a plurality of keys (i.e. multiple keys in triple DES where they are stored in ID register, in nonvolatile memory, page 2, paragraphs [0012], [0015], [0019-0021]); a configuration circuit (Fig. 5, element 12) coupled to the configuration memory and to the plurality of storage elements (Fig. 5, element 62), the configuration circuit adapted to configure the configuration memory with an input configuration bitstream (Fig. 5, elements 20, 64), wherein the configuration bitstream includes control data (Fig. 6, elements 80-84) and configuration data (Fig. 6, element 86) and at least the configuration data is encrypted (page 2, paragraph [0011]); and a decryptor (Fig. 5, element 64) coupled to the configuration circuit (Fig. 5, element 12) and to the plurality of storage elements (Fig. 5, element 62), the decryptor configured to decrypt, responsive to the configuration circuit, an input configuration bitstream using a plurality of decryption keys stored in the plurality of storage elements (Fig. 5, element 64; page 1, paragraph [0009]; page 8, paragraphs 0104-0107). Kean discloses the security circuit (Fig. 5, element 64) may encrypts/decrypts the configuration data using the triple data encryption standard algorithm (i.e. plurality of decryption keys) in a cipher block chaining (CBC) mode algorithm (page 2, paragraphs [0015] and [0023]). Kean further discloses cipher block chaining mode with the required initial value saved as part of the header before the configuration information (page 8, paragraphs [0107-0112] and in CBC decryption, the initial value is used for starting the chaining; and storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD page 7, paragraph [0095]).

Yip discloses decrypting the configuration bitstream in the PLD using the address from the configuration bitstream (page 3, paragraph [0031]; Fig. 2, element 48)

Kean does not disclose programmable logic circuitry coupled to the configuration memory.

The admitted prior art discloses programmable logic circuitry coupled to the configuration memory (Fig. 1, element 11).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of programmable logic circuitry coupled to the configuration memory as the admitted prior art discloses in the system of Kean and Yip, so as to provide programmable logic for PLD to perform desired functions.

b) As to claims 3, the admitted prior art discloses the initial address indicator is a frame address for indicating a starting frame of the PLD into which configuration data will be loaded (Fig. 2d, element 0001).

Allowable Subject Matter

9. Claims 5-6, 14-15, 19, 24-25 and 28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
4/14/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER